

## ISO 9001: Not a one-trick pony



### IN THIS ISSUE

Issue 601 of the Newsletter (the first issue this year) "celebrated" the end of the period between the release of ISO 9001:2000 in December 2000 and the final date of transition in December 2003.

The hope was that, with the end of this time of change, there was an opportunity for ISO Teams to use their Systems for the good of their organizations.

The ISO 9001 focus on continual improvement would provide the motivation. Certification bodies would cooperate by auditing performance as well as conformance.

Not everyone agreed that the ISO 9001 System was going to be a tool for progress. Some detractors focused on the "coercive" nature of many certifications and transitions ("you comply or we won't buy").

Having to certify rather than wanting to certify would limit management support to a minimum certification survival level.

Other critics pointed out that, even though the number of certified companies worldwide was increasing, certifications were actually falling in the "mature" ISO countries.

The increase was coming from companies in countries like China and Russia that were positioning themselves to meet a growing demand for "off shore" manufacturing. Potential customers encouraged manufacturers to certify to ISO 9001 to prove that they had the infrastructure necessary to consistently deliver quality product.

Incongruously, some of these outsourcers decided they no longer needed ISO 9001 themselves, because others were now doing their manufacturing

Are we back on the old merry-go-round? Companies certify because customers or interested parties coerce them. As a result, they do only what they have to do to gain and retain certification

Experience shows that, in many cases, this is still true. However, alternative motivations for certification are emerging.

QRC is dealing with companies that are implementing ISO 9001 to develop more robust and flexible business management systems. They are not being coerced.

The driving force for many of these companies is avoiding the risks inherent in running their organizations by "tribal knowledge"

Risks are everywhere:

⊗ Contract manufacturers, especially offshore ones, can present grave risks unless their processes meet known and verifiable standards.

Confirming the integrity of a manufacturers' system goes further than checking a certificate number.

To minimize risk, the customer needs the skills to establish the standards of performance required and verify that these standards are being achieved.

⊗ After the financial scandals of recent years, interested parties are at serious risk unless they can rely on accurate corporate disclosures.

The Sarbanes-Oxley Act of 2002 has been developed to address this need.

ISO Teams need to respond to the risks faced by their organizations.

There is little point in the ISO Team offering improvements that management does not think are necessary.

There is a real need to use the System to offer controls that management knows are essential.

In a W. C. Fields movie, the comedian was playing poker and was caught looking at the hand of the man next to him.

***"Isn't this a game of chance?" the man said.***

***"Not the way I play it" Fields replied.***



### SARBANES-OXLEY

Following the misdemeanors of companies like Enron and Global Crossing, the Sarbanes-Oxley Act of 2002 has become the poster child of risk prevention.

Applying to public companies that are subject to Securities laws, the Act describes its purpose as: "To protect investors by improving the accuracy and reliability of corporate disclosures."

**Newsletter 605**

The Sarbanes-Oxley Act has very sharp teeth. CEOs and CFOs are liable for severe penalties if their financial reports are not comprehensive and accurate.

These corporate leaders are required to ensure an adequate structure of internal controls that meet the standards for information set by the Act.

This Act is not a Standard, but Section 404 of the Act requires that management take responsibility for establishing and maintaining an adequate internal control structure that includes procedures for financial reporting.

Section 302 requires evaluation of these controls within 90 days of the preparation of financial reports.

We are examining this Act in a Newsletter for ISO Teams, because the needs of Sections 302 and 404 make it a lot like ISO 9001.

A good ISO Team understands processes and their evaluation. To install ISO 9001 it has been necessary to:

- 🏢 Identify the processes in the organization, and their interactions
- 🏢 Develop and document the processes needed to meet the requirements of the organization and the Standard.
- 🏢 Establish goals for the processes
- 🏢 Install the processes
- 🏢 Evaluate the processes
- 🏢 Correct nonconformities
- 🏢 Prove to a Third Party auditor that the processes are adequate to meet the objectives of the organization and the Standard.

The required steps to compliance to the Sarbanes-Oxley Act of 2002 have been described by the Knight-Ridder organization as:

1. List the key business processes
2. Describe the steps for each process
3. Describe the risks in each facet of the process
4. Describe the controls to lessen each risk.
5. Test whether the controls work in real life transactions
6. The CEO and CFO are to certify that the controls work
7. Prove to a Third Party Auditor that the processes are adequate to meet the control requirements of the Act"

The logistics of implementing and maintaining the requirements of Sarbanes-

Oxley and those of ISO 9001 are virtually the same. The primary difference is that:

- 🏢 ISO 9001 requires that *goals* be established and achieved
- 🏢 Sarbanes-Oxley requires that *risks* be established and avoided.

Companies that are using the QRC Protocol Method will already be familiar with including "Inputs", "Outputs" and "Goals" in the descriptions of their key processes.

It is a very small step to add "Risks" and "Safeguards" to these criteria.

In Newsletter 604, we illustrated the point that a "detached" manager would be unimpressed by an internal audit that reported calibration devices without stickers. The level of response from this manager would likely be very different if the audit finding was expressed as a possible warning of the need for a product recall.

ISO Teams can learn something from the Sarbanes-Oxley concentration on identifying and dealing with potential risk.

In ISO programs we develop processes after analyzing expected input and required output.

If we use input, output and *potential risk*, in this analysis, we could strengthen the process and make value added internal auditing more effective. The reports of negative audit findings would identify the risks that have been triggered.

This added dimension to audit reports would make them more likely to get the attention of the right people in and out of Management Review meetings.

***"It isn't that they can't see the solution. It is that they can't see the problem"***

G. K. Chesterton



**"DEJA VUE ALL OVER AGAIN"**

Yogi Berra

The implementation of Sarbanes-Oxley is reminiscent of the early implementations of ISO 9000:1987, and to a lesser extent, ISO 9000:1994.

In the late 1980s and early 1990s, Quality Managers were mostly chosen to implement the ISO Standards (it was a Quality System, after all).

There was uncertainty about what Certification Auditors would check.

**Newsletter 605**

Many installations embarked on a documentation overkill to make sure that all the bases were covered.

This gave rise to the opinion that ISO 9001 was a paperwork bureaucracy.

It took years to recover from that slur, and even now, the recovery is not complete.

Today, Financial managers (supported by Attorneys) are mostly chosen to implement the requirements of the Sarbanes-Oxley Act (it is a financial obligation with legal implications after all).

There is uncertainty how the Public Company Accounting Oversight Board (established by the Sarbanes-Oxley Act) will audit the control procedures of Corporations. Many organizations are embarking on a documentation overkill to make sure all bases are covered.

Already there are loud complaints about the amount of documentation required by the Act.

Those readers who worked with ISO in the early 1990s will also remember the teeth clenching costs of preparing for ISO Certification.

Whether developed internally, or with external help, the costs of implementing many ISO 9001 Systems were exorbitant. People were unsure of what needed to be done; so many people did a lot of stuff that didn't need to be done.

Distractions were everywhere. If some procedure in the organization was not "faultless" it would have to be changed. This stopped the program until the change was complete.

Then it was discovered that changing this procedure impacted other procedures, and so they too had to be changed.

As the changes multiplied, so did the costs. Top management felt it had no option but to grit their collective teeth and pay the bill.

Reports of the costs of preparing for the Sarbanes-Oxley audit would be perplexing, if there wasn't that ISO history with which to compare.

In all this repeating of history, organizations seem to be ignoring the fact that, over the past ten years, a group of processes have been developed and a team of people has gained experience that can make preparing for Sarbanes-Oxley a reasonable program in terms of cost and effort.

The group of processes is the ISO 9001 Quality Management System

The internal controls required by Sarbanes-Oxley are already partially in place in an ISO 9001 company (e.g. Purchasing; Control of Documents; Control of Records; Corrective Action; Preventive Action).

The areas that are not typically addressed (e.g. Cash Management) are far from daunting process development tasks.

The experienced people that can help respond to Sarbanes-Oxley are the ISO Team who already

- ☞ Understand processes
- ☞ Know how to set scopes for processes
- ☞ Know how to document processes
- ☞ Know how to install processes
- ☞ Know how to evaluate processes
- ☞ Know how to correct processes
- ☞ Understand how to successfully prepare for Third Party Audits

If the ISO Team is not operating the QRC Protocol Program, it will probably need to add the following to the affected processes

- ☞ Inputs: (to establish the source and quality of information and services to be received by the process)
- ☞ Outputs: (to establish the internal or external customer of the process and the quality of information and services required from the process)

- ☞ Goals: (to establish the required performance standards of the process)
- ☞ Risks: (to identify the consequences of not achieving the goals)
- ☞ Safeguards: (to establish the Preventive Actions taken to avoid the risk exposure)

This done, the Sarbanes-Oxley requirement will become part of the Business Management System, subject to:

- ☞ Evaluation (Internal Audit)
- ☞ Correction (Corrective Action)
- ☞ Risk Prevention (Preventive Action)
- ☞ Review (Management Review)
- ☞ Improvement (Continual Improvement)
- ☞ Third Party Review (Audit)

The ISO Team's knowledge is not limited to the ISO 9001 Standards. It includes skill sets that can be used in developing, implementing and evaluating any process based system. As with ISO 9001 installations, others have the technical knowledge, the ISO Team knows how to include that knowledge in a goal oriented, verifiable system.

***"When your work speaks for itself, don't interrupt"***

Henry J. Kaiser